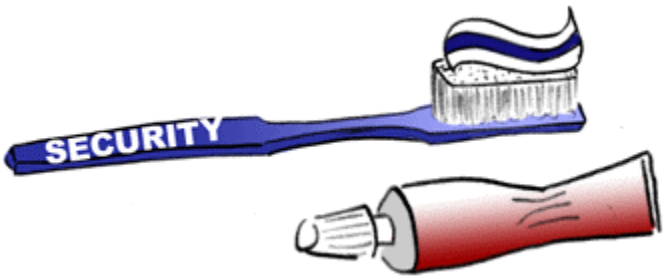
Security Quickie 12 – Awareness and Behavior

We all love to visit the dentist, right? Well… probably not. All of us like having healthy teeth and gums and sparkling smiles. Most dentists often have really great stories too, but nobody really likes sitting in ***The Chair*** and having their teeth poked and prodded with the sharp implements of dentistry while all they get to do is stare up at the ceiling and count the holes in those big ceiling tiles. As we grew up, all of us learned that in order to prevent cavities we needed to brush and floss our teeth every day, and generally watch out for certain types of foods. Then we were supposed to put that knowledge into effect and actually brush every day. Keeping your teeth healthy is a matter of education and ongoing behavior – it's a process, not just a single trip to the dentist.



Information Security is very much a process, too. The point of security is to mitigate risk – to keep systems secure, available, and working efficiently, in effect to keep information systems 'cavity free'. Security personnel help people learn the importance of 'brushing daily', that is, locking workstations, using strong passwords, and keeping confidential information safe. At times security personnel can be like a dentist by giving check-ups (Vulnerability Assessments), showing people how to brush and floss (Security Awareness), and when necessary fill cavities or perform root canals (Incident Response). Nobody really likes being in ***The Chair*** for serious surgery, however, and the best way to avoid that is to learn and practice good security behavior every day. Because unlike a cavity, an intrusion can happen from just one overlooked security procedure, like forgetting to lock a workstation, neglecting to patch a server's operating system, or setting an easy password. It is better by far to take the couple extra minutes every day to practice good security than it is to have to go through even one serious intrusion incident and get stuck in ***The Chair*** for a root canal. By brushing everyday and following security 'best-practices' we can have more dependable systems, have less intrusions, downtime, and data loss, and have more confidence in our sparkling information technology smile.

The Daily Regimen:

- Use strong passwords (change every 60 days) and protect them
- Lock your workstation when you leave it
- Shred confidential documents before throwing them away
- Scan new files, disks, and programs for malicious code
- Close or monitor all access doors
- When traveling, never leave equipment unattended
- Use good judgment when using the Internet